UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

DISH NETWORK L.L.C. and NAGRASTAR LLC, Plaintiffs, v. TIMOTHY SULLIVAN, Defendant.	Case No. **PLAINTIFFS' COMPLAINT**

Plaintiffs DISH Network L.L.C. ("DISH") and NagraStar LLC ("NagraStar," collectively "Plaintiffs") file this complaint against the above-named Defendant and state as follows:

PARTIES

1. Plaintiff DISH is a Colorado limited liability company with its principal place of business located at 9601 South Meridian Blvd., Englewood, Colorado 80112.

2. Plaintiff NagraStar is a Colorado limited liability company with its principal place of business located at 90 Inverness Circle East, Englewood, Colorado 80112.

3. Defendant Timothy Sullivan ("Defendant") is an individual believed to be residing at 17 Cross Street, Plympton, Massachusetts 02367.

JURISDICTION AND VENUE

4. This action alleges violations of the Digital Millennium Copyright Act, 17 U.S.C. § 1201 *et seq.*, the Federal Communications Act, 47 U.S.C. § 605 *et seq.*, and the Electronic Communications Privacy Act, 18 U.S.C. § 2511 *et seq.* Subject matter jurisdiction is proper in this Court pursuant to 28 U.S.C. §§ 1331 and 1338.

5. Defendant resides in and regularly conducts business in the State of Massachusetts, and therefore is subject to this Court's personal jurisdiction.

6. Venue is proper in this court under 28 U.S.C. § 1391(b)(1) because Defendant resides in this jurisdiction, § 1391(b)(2) because a substantial part of the events giving rise to Plaintiffs' claims occurred in this district, and § 1391(b)(3) because Defendant is subject to personal jurisdiction in this district. Venue is also proper in this Court under 28 U.S.C. § 1400(a) because this case asserts claims relating to the protection of copyrighted works.

NATURE OF THE ACTION[1]

7. On information and belief, Defendant has been trafficking in server passcodes that are designed and used solely for purposes of circumventing Plaintiffs' security system and receiving DISH's satellite broadcasts of copyrighted television programming without payment of the required subscription fee. Defendant is also believed to have personally used server passcodes to decrypt DISH's satellite signal and view DISH programming without authorization. Defendant's actions violate the Digital Millennium Copyright Act, Federal Communications Act, and Electronic Communications Privacy Act, as set forth below.

DISH'S SATELLITE TELEVISION PROGRAMMING

8. DISH uses high-powered satellites to broadcast television programming to millions of subscribers in the United States that pay DISH a subscription fee to receive such programming, or in the case of a pay-per-view program, the purchase price. NagraStar provides smart cards and other proprietary technologies that form a conditional access system used to authorize the subscribers' receipts of DISH's satellite communications of television programming.

[1] The allegations made by Plaintiffs concerning the whereabouts and wrongful conduct of Defendant are based on the investigation completed to date, and with the reasonable belief that further investigation and discovery in this action will lead to additional factual support. Plaintiffs reserve the right to supplement or amend their claims and the basis for those claims, with leave of the court if necessary, as additional investigation and discovery is conducted.

9. DISH contracts for and purchases the right to broadcast the television programming shown on its platform from networks, motion picture distributors, pay and specialty broadcasters, sports leagues, and other rights holders. DISH's subscribers enjoy access to hundreds of channels, including movie channels from HBO, Showtime, Cinemax, and Starz; sports channels from ESPN, NFL Network, MLB Network, and Willow Cricket; and other channels such as Discovery, A&E, Disney, TNT, TBS, USA, BET, and Bravo, among many others (the "DISH Programming").

10. The works broadcast by DISH are copyrighted. Plaintiffs have the authority of the copyright holders to protect the works from unauthorized reception and viewing.

11. DISH programming is digitalized, compressed, and scrambled prior to being transmitted to multiple satellites located in geo-synchronous orbit above Earth. The satellites, which have relatively fixed footprints covering the United States and parts of Canada, Mexico, and the Caribbean, relay the encrypted signal back to Earth where it can be received by DISH subscribers that have the necessary equipment.

12. A DISH satellite television system consists of a compatible dish antenna, receiver, smart card which in some instances is internalized in the receiver, television, and cabling to connect the components. DISH provides receivers, dish antenna, and other digital equipment for the DISH system. Smart cards and other proprietary security technologies that form a conditional access system are supplied by NagraStar.

13. Each DISH receiver and NagraStar smart card is assigned a unique serial number that is used by DISH when activating the equipment and to ensure the equipment only decrypts programming the customer is authorized to receive as part of his subscription package and pay-per-view purchases.

14. The NagraStar conditional access system performs two interrelated functions in the ordinary course of its operation: first, subscriber rights management, which allows DISH to "turn on" and "turn off" programming a customer has ordered, cancelled, or changed; and second, protection of the NagraStar control words that descramble DISH's satellite signal, which in turn prevents unauthorized decryption of DISH programming.

15. An integral part of NagraStar's conditional access system is a smart card having a secure embedded microprocessor. The DISH receiver processes an incoming DISH satellite signal by locating an encrypted part of the transmission known as the NagraStar entitlement control message and forwards it to the smart card. Provided the subscriber is tuned to a channel he is authorized to watch, the smart card uses its decryption keys to unlock the message, uncovering a control word. The control word is then transmitted back to the recover to decrypt the DISH satellite signal.

16. Together, the DISH receiver and NagraStar smart card convert DISH's encrypted satellite signal into viewable programming that can be displayed on the attached television of an authorized DISH subscriber.

PIRACY OF DISH NETWORK PROGRAMMING

17. The term "piracy" (or signal theft) is used throughout the pay-tv industry to refer to the circumvention of security technology protecting a pay-tv signal and/or the unauthorized reception, decryption, or viewing of a pay-tv signal. A form of satellite piracy exists that goes by several names including "control word sharing," "Internet key sharing," or more simply "IKS."

18. With IKS, once piracy software is loaded onto an unauthorized receiver, the end user connects the receiver to the Internet via a built-in Ethernet port or an add-on dongle. The

Internet connection automatically updates piracy software on the receiver and contacts a computer server that provides the necessary control words.

19. The computer server, called and "IKS server," has multiple, subscribed NagraStar smart cards connected to it, and thus the ability to provide the control words. Access to an IKS server typically requires a valid passcode. Once access has been obtained, control words are sent from the IKS server over the Internet to an unauthorized receiver, where they are used to decrypt DISH's signal and view programming without paying a subscription fee.

DEFENDANT'S WRONGFUL CONDUCT

20. NFusion Private Server ("NFPS") is a subscription-based IKS service, whereby members purchase a subscription to the IKS service to obtain the control words that are used to circumvent Plaintiffs' security system and receive DISH's satellite broadcasts of television programming without authorization.

21. Digital TV is a Dominican Republic company that sold subscriptions to NFPS. ("IKS Server Passcodes"). Digital TV provided Plaintiffs with copies of its business records pertaining to Defendant. Digital TV's records show that Defendant purchased at least 11 IKS Server Passcodes within the statute of limitations for each claim that Plaintiffs are bringing against Defendant. Each IKS Server Passcode that Defendant purchased is believed to have been valid for a one year period of time.

22. On information and belief, Defendant re-sold certain IKS Server Passcodes that he purchased from Digital TV. These IKS Server Passcodes enabled Defendant's customers to access the NFPS service using an unauthorized receiver loaded with piracy software. Each time that the customer tuned their unauthorized receiver to an encrypted DISH channel, the receiver requested the control word for that particular channel from the IKS server. The IKS servers then

returned Plaintiffs' control word, which the customer used to decrypt DISH's satellite signal and view DISH programming without purchasing a subscription from DISH.

23. On information and belief, Defendant also used certain IKS Server Passcodes that he purchased for his own personal benefit. Defendant is believed to have used an IKS Server Passcode in connection with an unauthorized receiver loaded with piracy software to access the IKS service. Each time Defendant tuned the unauthorized receiver to an encrypted DISH channel, the receiver requested the control word for that particular channel from the IKS server. The IKS server then returned the control word to Defendant, which he used to decrypt DISH's satellite signal and view DISH programming without purchasing a subscription from DISH.

24. Defendant's actions cause actual and imminent irreparable harm for which there is no adequate remedy at law. Through IKS piracy, Defendant has unlimited access to DISH programming, including premium and pay-per-view channels, causing lost revenues that cannot be fully calculated. In addition, Defendant's actions damage the business reputations and goodwill of Plaintiffs, and result in the need for costly and continuous security updates, investigations, and legal actions aimed at stopping satellite piracy.

CLAIMS FOR RELIEF

COUNT I

Trafficking in Circumvention Technology and Services in Violation of the Digital Millennium Copyright Act, 17 U.S.C. § 1201(a)(2)

25. Plaintiffs repeat and reallege the allegations in paragraphs 1-24.

26. On information and belief, Defendant has been importing, offering to the public, providing, or otherwise trafficking in IKS Server Passcodes in violation of 17 U.S.C. § 1201(a)(2).

27. The IKS Server Passcodes are primarily designed and produced for circumventing Plaintiffs' security system; have no commercially significant purpose or use other than to circumvent Plaintiffs' security system; and on information and belief are marketed by Defendant and others known to be acting in concert for use in circumventing Plaintiffs' security system.

28. Plaintiffs' security system is a technological measure that effectively controls access to, copying, and distribution of copyrighted works. Defendant's actions that constitute violations of 17 U.S.C. § 1201(a)(2) were performed without permission, authorization, or consent from DISH, NagraStar, or any owner of the copyrighted programming broadcast by DISH.

29. Defendant violated 17 U.S.C. § 1201(a)(2) willfully and for purposes of commercial advantage and private financial gain. Defendant knew or should have known his actions are illegal and prohibited.

30. Defendant's violations cause damage to Plaintiffs in an amount to be proven at trial. Unless restrained and enjoined by the Court, Defendant will continue to violate 17 U.S.C. § 1201(a)(2).

COUNT II

Distributing Signal Theft Devices and Equipment in Violation of the Federal Communications Act, 47 U.S.C. § 605(e)(4)

31. Plaintiffs repeat and reallege the allegations in paragraphs 1-24.

32. On information and belief, Defendant has been importing, assembling, selling, or otherwise distributing IKS Server Passcodes in violation 47 U.S.C. § 605(e)(4).

33. The IKS Server Passcodes are primarily of assistance in decrypting DISH's satellite transmissions of television programming without authorization. Defendant intended for the IKS Server Passcodes to be used for this purpose.

34. Defendant violated 47 U.S.C. § 605(e)(4) willfully and for the purposes of commercial advantage and private financial gain. Defendant knew or should have known his actions are illegal and prohibited.

35. Defendant's violations cause damage to Plaintiffs in an amount to be proven at trial. Unless restrained and enjoined by the Court, Defendant will continue to violate 47 U.S.C. § 605(e)(4).

COUNT III

Circumventing an Access Control Measure in Violation of the Digital Millennium Copyright Act, 17 U.S.C. § 1201(a)(1)

36. Plaintiffs repeat and reallege the allegations in paragraphs 1-24.

37. Defendant has been circumventing Plaintiffs' security system in violation of 17 U.S.C. § 1201(a)(1) by the acts set forth above, including his receipt of Plaintiffs' control words from NFPS, and his use of those pirated control words to decrypt DISH's satellite transmissions of television programming.

38. Plaintiffs' security system is a technological measure that effectively controls access to, copying, and distribution of copyrighted works. Defendant's actions that constitute violations of 17 U.S.C. § 1201(a)(1) were performed without the permission, consent, or authorization of DISH, NagraStar, or any owner of the copyrighted programming broadcast on the DISH platform.

39. Defendant violated 17 U.S.C. § 1201(a)(1) willfully and for the purpose of commercial advantage or private financial gain.

40. Defendant knew or should have known his actions were illegal and prohibited. Such violations have and will continue to cause damage to Plaintiffs in an amount to be proven at trial. Unless restrained and enjoined by the Court, Defendant will continue to violate 17 U.S.C. § 1201(a)(1).

COUNT IV

Receiving Satellite Signals Without Authorization in Violation of the Federal Communications Act, 47 U.S.C § 605(a)

41. Plaintiffs repeat and reallege the allegations in paragraphs 1-24.

42. Through NFPS, Defendant has been receiving Plaintiffs' control words and DISH's satellite transmissions of television programming for his own benefit and without authorization in violation of 47 U.S.C. § 605(a).

43. Defendant violated 47 U.S.C. § 605(a) willfully and for purposes of commercial advantage or private financial gain.

44. Defendant knew or should have known his actions were illegal and prohibited. Such violations have and will cause damage to Plaintiffs in an amount to be proven at trial. Unless restrained and enjoined by the Court, Defendant will continue to violate 47 U.S.C. § 605(a).

COUNT V

Intercepting Satellite Signals in Violation of the Electronic Communications Privacy Act, 18 U.S.C. §§ 2511(1)(a) and 2520

45. Plaintiffs repeat and reallege the allegations in paragraphs 1-24.

46. Through NFPS, Defendant has been intercepting Plaintiffs' control words and DISH's satellite transmissions of television programming in violation of 18 U.S.C. §§ 2511(1)(a) and 2520.

47. Defendant violated 18 U.S.C. §§ 2511(1)(a) and 2520 for tortious and illegal purposes, or for commercial advantage or private gain.

48. Defendant's interception was intentional, and therefore illegal and prohibited. Such violations have and will continue to cause damage to Plaintiffs in an amount to be proven at trial. Unless restrained and enjoined by the Court, Defendant will continue to violate 18 U.S.C. §§ 2511(1)(a) and 2520.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs seek judgment against Defendant as follows:

A. For a grant of permanent injunctive relief restraining and enjoining Defendant, and his employees, agents, representatives, attorneys, and all persons acting or claiming to act on his behalf or under his direction or authority, and all persons acting in concert or participation with him, from:

(1) manufacturing, importing, offering to the public, providing, or trafficking in IKS Server Passcodes, and any other technology, product, service, device, component, or part therefore that:

(a) is primarily designed or produced for circumventing Plaintiffs' security system or any other technological measure adopted by Plaintiffs that controls access to, copying, or the distribution of copyrighted works on the DISH platform;

(b) has only a limited commercially significant purpose or use other than to circumvent Plaintiffs' security system or any other technological measure adopted by

Plaintiffs that controls access to, copying, or the distribution of copyrighted works on the DISH platform; or

(c) is marketed for use in circumventing Plaintiffs' security system or any other technological measure adopted by Plaintiffs that controls access to, copying, or the distribution of copyrighted works on the DISH platform;

(2) manufacturing, assembling, modifying, importing, exporting, selling, or distributing IKS Server Passcodes or any other product knowing or having reason to know that such product is primarily of assistance in the unauthorized decryption of direct-to-home satellite services;

(3) circumventing Plaintiffs' security system, or assisting others to circumvent Plaintiffs' security system;

(4) intercepting or otherwise receiving DISH's satellite transmissions of television programming without authorization, or assisting or procuring others to intercept or receive DISH's satellite transmissions of television programming without authorization;

B. For an order impounding, and authorizing Plaintiffs to take possession of and destroy, all IKS Server Passcodes, unauthorized receivers, piracy software, and any other devices, components, or parts thereof that are in the custody or control of Defendant and which the Court has reasonable cause to believe were involved in a violation of the Digital Millennium Copyright Act, 17 U.S.C. § 1201, or the Federal Communications Act, 47 U.S.C. § 605;

C. For an order directing Defendant to preserve and turn over to Plaintiffs all hard copy and electronic records that evidence, refer, or relate to IKS Server Passcodes or any other product that is used in satellite television piracy, including the manufacturers, exporters,

importers, dealers, or purchasers of such products, or persons otherwise involved in operating any IKS server or receiving control words from same;

D. Award Plaintiffs the greater of their actual damages together with any profits made by Defendant that are attributable to the violations alleged herein, or statutory damages in the amount of up to $2,500 for each violation of 17 U.S.C. §§ 1201(a)(1) and 1201(a)(2), under 17 U.S.C. §§ 1203(c)(2) and 1203(c)(3)(A);

E. Award Plaintiffs the greater of their actual damages together with any profits made by Defendant that are attributable to the violations alleged herein, or statutory damages in the amount of up to $100,000 for each violation of 47 U.S.C. § 605(e)(4), under 47 U.S.C. § 605(e)(3)(C)(i);

F. Award Plaintiffs the greater of their actual damages together with any profits made by Defendant that are attributable to the violations alleged herein, or statutory damages in the amount of up to $10,000 for each violation of 47 U.S.C. § 605(a), under 47 U.S.C. § 605(e)(3)(C)(i). Plaintiffs ask the Court to increase the amount by $100,000 for each violation, at the Court's discretion, in accordance with 47 U.S.C. § 605(e)(3)(C)(ii);

G. Award Plaintiffs the greater of their actual damages together with any profits made by Defendant that are attributable to the violations alleged herein, or statutory damages in the amount of $100 per day for each violation of 18 U.S.C. §§ 2511(1)(a) or $10,000, under 18 U.S.C. § 2520(c)(2);

H. Award Plaintiffs punitive damages under 18 U.S.C. § 2520(b)(2);

I. Award Plaintiffs their costs, attorney's fees, and investigative expenses under 17 U.S.C. § 1203(b)(4)-(5), 47 U.S.C. § 605(e)(3)(B)(iii), and 18 U.S.C. § 2520(b)(3);

J. For pre and post-judgment interest on all damages, from the earliest date permitted by law at the maximum rate permitted by law; and

K. For such additional relief as the Court deems just and equitable.

Dated: April 24, 2020

Respectfully submitted,

/s/ Patricia A. Szumowski
Patricia A. Szumowski BBO #653839
SZUMOWSKI LAW, P.C.
417 West Street, Suite 104
P.O. Box 2537
Amherst, MA 01004
Tel: (413) 835-0956
Fax: (866) 242-2902
pas@szumowskilaw.com

Attorneys for Plaintiffs DISH Network L.L.C. and NagraStar LLC

CERTIFICATE OF SERVICE

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) and paper copies will be sent to those indicated as non-registered participants on the NEF.

Dated: April 24, 2020

/s/ Patricia A. Szumowski
Patricia A. Szumowski